



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,659	10/16/2003	Tien-Shin Ho	REAP0013USA	2658
27765	7590	11/14/2006	EXAMINER	
NORTH AMERICA INTELLECTUAL PROPERTY CORPORATION P.O. BOX 506 MERRIFIELD, VA 22116				NALVEN, ANDREW L
ART UNIT		PAPER NUMBER		
		2134		

DATE MAILED: 11/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/605,659	HO ET AL.
	Examiner Andrew L. Nalven	Art Unit 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 16 October 2003.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-15 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-15 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 16 October 2003 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-15 are pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. **Claims 1 and 10-11 are rejected under 35 U.S.C. 101** because the claimed invention is directed to non-statutory subject matter. The cited apparatus claims may be interpreted as being directed to purely software components. Thus, the cited apparatus claims fail to provide a tangible element.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. **Claims 1-15 are rejected under 35 U.S.C. 112, second paragraph,** as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1-15 provide for the calculating of a TKIP Sbox value in accordance with the "IEEE P803.11i specification." A reference to the IEEE specification is indefinite because specifications may change over time as they

are modified and evolve. Hence, it is indefinite as to what Applicant is attempting to claim as their invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. **Claims 1-15 are rejected under 35 U.S.C. 102(a)** as being anticipated by Tom St. Denis "Analysis of TKIP Temporal Key Integrity Protocol (hereafter "Denis").

5. **With regards to claims 1, 6 and 11,** Denis teaches a first plurality of combinatorial logic for calculating a TKIP Sbox left value according to a low part of an index value (Denis, pages 4-5 sections 3 and 3.1, Figure 3, x0), a second plurality of combinatorial logic for calculating a TKIP Sbox right value according to a high part of the index value (Denis, pages 4-5 sections 3 and 3.1, Figure 3, x1), and a third plurality of combinatorial logic for calculating the TKIP Sbox value according to the TKIP Sbox left value and the TKIP Sbox right value (Denis, pages 4-5 sections 3 and 3.1, Figure 3).

6. **With regards to claims 2 and 12,** Denis teaches the third plurality of combinatorial logic is a plurality of XOR gates (Denis, Figure 3.1).

7. **With regards to claims 3, 7 and 13,** Denis teaches the TKIP Sbox left value is XORed with the TKIP Sbox right value by the plurality of XOR gates and the output of the plurality of XOR gates forms the TKIP Sbox value (Denis, Figure 3.1).
8. **With regards to claim 4, 8 and 14,** Denis teaches that for each bit in the TKIP Sbox left value, the first plurality of combinatorial logic comprises a logic circuit, each logic circuit respectively calculating a bit in the TKIP Sbox left value (Denis, pages 4-5 sections 3 and 3.1, Figure 3).
9. **With regards to claims 5, 9 and 15,** Denis teaches that for each bit in the TKIP Sbox right value, the first plurality of combinatorial logic comprises a logic circuit, each logic circuit respectively calculating a bit in the TKIP Sbox right value (Denis, pages 4-5 sections 3 and 3.1, Figure 3).
10. **With regards to claim 10,** Denis teaches TKIP Sbox logic configured to calculate a TKIP Sbox value according to an index value (Denis, Figure 3.1).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

11. Benoit US Patent No. 6,820,814 discloses a countermeasure method in an electric component using a secret key cryptographic algorithm.
12. Adams et al US Patent No. 5,825,886 discloses a symmetric cipher using the cast design procedure.

Art Unit: 2134

13. Swinglehurst et al US PGPub 2003/0091185 discloses a key stream cipher device.

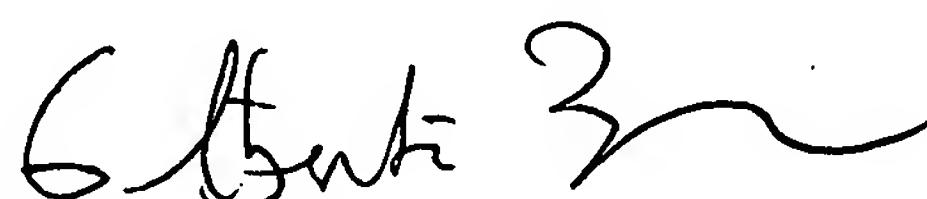
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571 272 3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Andrew Nalven

AN



GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100